Les "Safe Harbor Principles"

Poullet, Yves

Published in:
Le droit de l'Informatique au tournant du Millénaire

Publication date:
2000

Document Version
le PDF de l'éditeur

L'ASBL

http://www.droit-technologie.org

http://www.juriscom.net

présentent :

Les Safe Harbor Principles - Une protection adéquate ?

Yves Poullet

Yves.poullet@fundp.ac.be
Professeur à la faculté de Droit de Namur (FUNDP)
Directeur du CRID

10/07/2000

Introduction

1. La « globalisation » de l'économie, la dimension internationale croissante de nos réseaux de télécommunications mettent au centre des soucis de protection des données le phénomène des flux transfrontières et les risques encourus par les citoyens du fait de la disparité, voire de l'absence des régimes de protection des données dans les pays tiers.

Quatre exemples témoignent de cette réalité croissante :

2. Le premier exemple (1) est la création par une multinationale américaine disposant de sièges en Europe d'une banque de données relatives au personnel de cadre, où qu'il soit, et recensant des renseignements de tous ordres : ambitions, formation reçue, hobbies… Il s'agit, pour cette multinationale, de pouvoir répondre facilement à des besoins internes de la compagnie comme celui de la constitution d'équipes de prospection d'un nouveau marché, de la recherche de formateurs, voire de la création d'une équipe sportive. Ces données collectées à partir de multiples sources – formulaires ou interviews lors des candidatures, appréciation par des supérieurs hiérarchiques, participation à des cycles de formation – sont en l'occurrence assemblées et envoyées à partir de lieux divers (centres de formation, directions du personnel des différentes entités locales…) aux services centraux de direction du personnel de la multinationale. La banque de données localisée au siège central de la multinationale est accessible par les différents sièges locaux.

3. La délocalisation d'activités dans des pays du tiers monde suggère un deuxième exemple (2) : soit une entreprise belge de listes d'adresses travaillant sur les marchés belges et hollandais et décidant de sous-traiter l'ensemble de ses activités d'encodage, de triage ou encore de sélection, dans un pays africain. Les données sont collectées principalement auprès de la personne concernée à partir d'un vaste questionnaire portant sur les habitudes de consommation (voyages, alimentation, culture…). Elles sont croisées avec d'autres données : numéro de téléphone, importance de la localité, type de quartier (revenu moyen par habitant, etc.) provenant de sources publiques accessibles directement de l'étranger ou transférées par support informatique. Les données sont exceptionnellement transmises directement d'Afrique à un autre pays tiers, où un client de l'entreprise belge désire tester auprès d'un échantillon représentatif contacté par publipostage ou par téléphone l'intérêt pour un produit que cette entreprise étrangère s'apprête à lancer sur le marché belge.

4. Le troisième exemple (3) est celui de grands systèmes informatisés de réservation aérienne. L'un des plus importants d'entre eux est localisé pour les cinq continents aux Etats-Unis et gère quotidiennement 2.000.000 réservations venant du monde entier. Cela signifie que chaque jour, chaque seconde, des données à caractère personnel sont traitées par cette société. Ces données sont enregistrées sous forme de « *Passenger Name Record* » (ou PNR). Outre le nom et l'adresse des passagers, ces PNR contiennent leurs destinations aériennes, leur état de fumeur ou non, parfois les hôtels qu'ils choisissent, les voitures qu'ils louent ou encore leur numéro de carte de crédit.

5. Enfin (4), les exemples liés au phénomène Internet appellent la remarque suivante : la mise sur un site d'une information nominative ou d'un message destiné à un forum de discussion ouvert, même si elle a pour l'émetteur une finalité déterminée, permet à cette information ou à ce message d'être utilisés pour de multiples finalités par la variété indéterminée de personnes ayant accès à ces informations. Ainsi, un *curriculum vitae* mis sur Internet peut être utilisé par des employeurs potentiels, des sociétés de *marketing*, d'autres chercheurs d'emploi, une administration de sécurité sociale, voire une secte… Le phénomène des *cookies* peut être également cité ici. L'affaire *DoubleClick*[1] est exemplative à ce propos. Cette société américaine qui compte plus de 11.500 sites affiliés collecte les informations générées par les *cookies*[2] auprès de plus de cent millions d'internautes dont nombreux sont européens. Cette collecte et le profilage des internautes qu'elle entraîne permettent à *DoubleClick* de sélectionner de manière adéquate les "*banners*" publicitaires et de transmettre aux tiers des informations utiles pour leur propre *marketing* ou la sélection des pages web appropriées lors de la visite des internautes.

6. C'est dans ce contexte d'intensification des flux transfrontières, en particulier entre l'Europe et les Etats Unis[3], que, pour apaiser l'inquiétude européenne à propos du respect de la protection des données offert lors de tels transferts, les Etats Unis proposent un système original de protection des données, qualifié habituellement de *Safe Harbor Principles*, traduisible littéralement par « principes du port sûr ».

7. Ce système reprend, selon le sous-titre même, des « *Elements of Effective selfregulation for privacy Protection* ». En d'autres termes, le système américain proposé repose sur une solution d'autoréglementation et non sur une solution législative. En réalité, le fait que le *Department of Commerce* américain soit à l'origine de ces *Safe Harbor Principles* et le constat suivant lequel « *l'effectivité de ces principes dépend d'organes juridictionnels officiels, en particulier de la Federal Trade Commission* » plaideraient pour y voir non une autoréglementation an sens strict mais, selon la qualification récemment retenue par les débats de l'OCDE[4], un « *effective mix* », c'est-à-dire un système alliant les vertus de l'autoréglementation et l'autorité de la puissance publique.

8. L'objet de notre étude porte donc sur le caractère adéquat de la protection offerte par les Etats Unis dans le cadre de ces *Safe Harbor Principles*. Elle s'ajoute à de nombreux

[1] Une plainte a été récemment introduite par l'*EPIC* contre *DoubleClick* auprès de la F.T.C. et ceci après le rachat par *DoubleClick* de la société *Abacus*, spécialisée en marketing direct (sur cette plainte, cf. le site de l'*EPIC* : <http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf>). Grâce à ce rachat, la société peut en effet individualiser les internautes non plus seulement par l'identifiant du *Cookie* mais, le cas échéant, par leur nom.

[2] Sur les méthodes de collecte de ces informations grâce à des liens invisibles à partir des sites affiliés, lire J-M. Dinant, « Les traitements invisibles sur Internet », *CRID*, <http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html > cf. également, S. Gauthronet et F. Nathan, *Les services en ligne et la protection des données ou de la vie privée*, étude pour la D.G. XV, disponible sur le site *Europa* : <http://www.europa.eu.int/commm/dg15/en /media/dataprot/studies/servint.htm>.

[3] A noter plus récemment, l'affaire Echelon, c'est-à-dire l'écoute systématique par la NSA américaine des télécommunications transitant par satellites. Cette affaire illustre un autre danger pour les citoyens européens des pratiques américaines cette fois vis-à-vis des autorités américaines de sûreté de l'Etat (Sur cette affaire, le rapport présenté au Sénat belge par l'auteur et J-M. Dinant, *Le Réseau Echelon, faut-il s'en méfier ?*, à paraître).

[4] Voir à ce propos les débats tenus lors de la conférence de suivi d'Ottawa sur le commerce électronique (Paris, novembre 1999). Sur la notion d'autorégulation, lire en particulier les travaux de la Fondation Bertelsman.

commentaires déjà émis par le Groupe européen dit de l'article 29, Groupe des représentants des autorités nationales de protection des données, et au projet de décision de la Commission européenne relative à la pertinence des principes américains[5].

9. L'étude rappelle, dans un premier temps, le prescrit de l'article 25, analyse ensuite le mécanisme prévu par les Etats Unis et l'état actuel du dialogue « U.S. / E.U. » et, enfin, étudie le contenu même des principes et leur « *enforcement* » au regard des exigences de l'article 25. De brèves conclusions clôturent le discours.

[5] Projet du 17 mars soumis au Comité dit de l'article 31 lors de la réunion de ce dernier les 30 et 31 mars 2000, projet de décision de la Commission relative « à la pertinence des principes de la sphère de sécurité publiés par les Etats-Unis ».

I. Rappel des principes de l'article 25 de la Directive 95/46/CE en matière de flux transfrontaliers

10. L'article 25 paragraphe 1 de la Directive fait obligation aux Etats membres de veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays en question assure un niveau de protection adéquat et si les lois nationales qui mettent en œuvre d'autres dispositions de la Directive sont respectées avant le transfert.

11. L'article 25 paragraphe 6 de la Directive permet à la Commission, assistée du comité établi en vertu de l'article 31, de constater qu'un pays tiers assure un niveau de protection adéquat. Cette constatation permet de transférer des données à caractère personnel depuis les Etats membres sans que des garanties supplémentaires soient nécessaires. Il est souhaitable, lorsque cela est justifié, de faire de telles constatations afin d'assurer la sécurité juridique et de simplifier les procédures que doivent suivre les responsables des traitements de données qui envisagent de transférer des données vers des pays tiers. Pour les mêmes raisons, ces constatations doivent, si possible, couvrir toutes les activités rentrant dans le champ d'application de la Directive, parmi lesquelles figurent les télécommunications, pour lesquelles la Directive est précisée et complétée par la Directive 97/66/CE (J.O., L 24 du 30 janv. 1998, p. 1).

12. L'article 25 paragraphe 2 de la Directive dispose que le niveau de protection des données s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et qu'il est tenu compte, en particulier, des règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées. Le groupe de travail établi en vertu de l'article 29 de la Directive a formulé des indications sur la manière de mener cette évaluation[6]. Nous reviendrons amplement sur ces indications lors de l'analyse des principes américains.

II. Présentation des *Safe Harbor Principles*

13. En réaction à la Directive européenne et à ses exigences, le *Department of Commerce* américain en particulier la *National Information Agency* ont rapidement affirmé que la volonté américaine était, en ce qui concerne du moins le secteur privé, d'assurer une protection adéquate dans le cadre non d'une législation[7] mais de codes de conduite et

[6] Il s'agit du document de travail : *Transferts de données à caractère personnel à des pays tiers : application des articles 25 et 26 de la directive européenne relative à la protection des données*, document adopté le 24 juillet 1998. Ce document reprend les conclusions de l'étude menée par le *CRID* en 1996 et 1997 : Y. Poullet et B. Havelange, *Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement des traitements de données à caractère personnel*, Commission européenne, Annexe au rapport annuel du groupe de travail de l'article 29, 1998, Luxembourg, Office des publications officielles, ISBN 92-828-4304, 1998.

[7] Le récent rapport au Congrès de la *Federal Trade Commission* plaide clairement pour l'adoption d'une législation aux Etats-Unis dans les termes suivants (p. 36) : « Ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumer's privacy on the Internet. Accordingly, the Commission recommends that Congress enact legislation to ensure adequate protection of consumer privacy online. In doing so, however, the Commission recognizes that industry self-regulation, as well as consumer and business education, should still play important roles in any

autres instruments d'autorégulation. Un premier texte qualifié d'« *Elements of Effective selfregulation for privacy Protection* » a été publié à ce propos en 1998. Suite aux négociations ininterrompues depuis 1998 entre la Commission européenne[8] et les Etats-Unis, la position américaine a largement évolué. Le *Department of Commerce* du gouvernement américain a publié diverses versions des *Safe Harbor Principles* ou, selon la traduction française, des « *principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée* », qui visent à assurer la protection des données à caractère personnel transférées d'un Etat membre européen vers les Etats-Unis[9]. La dernière version a été publiée le 17 mars. Par ailleurs, ces principes sont complétés par la réponse à des « QFP » ou, selon la terminologie américaine utilisée, à des « FAQ » (Questions Fréquemment Posées = *Frequently Asked Questions*), publiées par le Ministère du Commerce des Etats-Unis et fournissant des orientations pour la mise en œuvre de ces principes.

14. Pour l'essentiel, les principes publiés et les FAQ réaffirment l'essentiel des « *Elements of Effective selfregulation for privacy Protection* » même si de notables progrès en ce qui concerne le contenu et l'« effectivité » (*enforcement*) des principes doivent être notés. On remarquera tout d'abord que les *Safe Harbor Principles* ne concernent pas les données « purement américaines », c'est-à-dire celles collectées auprès de citoyens américains aux Etats-Unis, et donc non protégées à l'origine par la Directive. Ce point est important. On déplorera avec nombre d'auteurs d'outre atlantique que les principes y repris ne puissent être invoqués par des citoyens américains mais, plus grave, on s'interrogera sur l'effectivité des principes dans la mesure où les entreprises américaines devront soumettre les données d'origine européenne à d'autres règles que celles habituellement suivies vis-à-vis des données majoritaires, les données purement américaines. Il va de soi que

---

legislative framework, as they have in other contexts. The proposed legislation would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites to the extent not already provided by the COPPA. Such legislation would set out the basic standards of practice governing the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards. » ; *Privacy online: Fair Information practices in the Electronic marketplace*, mai 2000, document disponible sur le site de la *Federal Trade Commission* :
<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

[8] Le Groupe dit de l'article 29 a émis dans le cadre de ces négociations et à propos des diverses versions du texte du *Safe Harbor* les opinions suivantes :
- Opinion 1/99 du 26 janvier 1999 – W.P. 15
- Opinion 2/99 du 3 mai 1999 – W.P. 19
- Opinion 4/99 du 7 juin 1999 – W.P. 21

Auxquelles s'ajoute le document de travail du 7 juillet 1999 – W.P. 23
- Opinion 7/99 du 3 décembre 1999 – W.P. 27.

[9] On note que les *Safe Harbor Principles* ne concernent pas les données purement « américaines », c'est-à-dire non protégées à l'origine par la Directive. Ce point est important. On déplorera avec nombre d'auteurs américains que les principes y repris ne puissent être invoqués par des citoyens américains mais, plus grave, on s'interrogera sur l'effectivité des principes dans la mesure où les entreprises américaines devront soumettre les données d'origine européenne à d'autres règles que celles habituellement suivies. Il va de soi que l'uniformité des règles en vigueur, quelle que soit l'origine, eût été préférable et non la soumission à des règles différentes, ce qui entraîne des risques de méconnaissance des règles du *Safe Harbor* au sein des organisations américaines. Un exemple est la question de la définition des données sensibles singulièrement élargie par les *Safe Harbor Principles* par rapport à la définition américaine classique. Spontanément, un employeur américain ne rangera pas comme donnée sensible l'opinion syndicale ou la donnée d'origine ethnique de son employé.

l'uniformité des règles en vigueur quelle que soit l'origine eût été préférable et non la soumission à des règles différentes, ce qui entraîne des risques de méconnaissance des règles du *Safe Harbor* au sein des organisations américaines. Un exemple est la définition des données sensibles reprises par le *Safe Harbor*. Cette définition, même si elle ne satisfait pas le prescrit européen, est bien plus large que celle communément admise aux Etats-Unis : ainsi la race est une donnée sensible au sens du *Safe Harbor* et non de la législation américaine. On peut donc craindre qu'un employeur américain ne range pas spontanément la race comme donnée sensible. En d'autres termes, le fait que le *Safe Harbor* soit une législation d'exception laisse craindre une moindre effectivité des règles y contenues.

15. L'adhésion à ces principes est totalement volontaire. Cependant, pour que les organisations obtiennent et conservent la reconnaissance du fait qu'elles assurent un niveau de protection adéquat pour le transfert de données de l'Union européenne vers les Etats-Unis conformément à la présente décision, elles doivent souscrire à ces principes, divulguer leurs règles de confidentialité et relever de la compétence de la Commission fédérale du commerce en vertu des dispositions de la section 5 du « *Federal Trade Commission Act* » qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce ou de tout autre organisme remplissant une mission analogue.

16. Le « *Federal Trade Commission* Act » permet à la Commission fédérale du commerce[10] d'obtenir des mesures de redressement par voie d'injonction en cas de pratiques déloyales ou frauduleuses et la réparation des préjudices subis par les citoyens des Etats-Unis ou d'autres pays ; dans l'exercice de ses fonctions officielles de contrôle dans son domaine de compétence. La F.T.C. a en outre montré qu'elle était disposée à étudier les plaintes indépendamment de la nationalité ou du pays de résidence du plaignant.

17. Enfin, on note que la F.T.C., suite à une demande d'explications de la Commission, a adressé le 29 mars 2000 un courrier à Monsieur J. Mogg, Directeur de la DG Marché Intérieur, dans lequel elle explicite l'étendue de ses compétences[11].

18. La Commission européenne a soumis au Comité de l'article 31, lors de sa réunion des 30 et 31 mars, un projet de décision de la Commission relative « *à la pertinence des principes de la sphère de sécurité publiés par les Etats-Unis* » (projet du 17 mars). Ce projet de décision rappelle les limites de la compétence de la *Federal Trade Commission* et estime que « *La 'sphère de sécurité' créée par les principes, si elle s'appuie sur des mécanismes publics et privés bien établis aux Etats-Unis, représente néanmoins une approche novatrice qui devra peut-être être revue à la lumière de l'expérience et des*

[10] Ci-après F.T.C. (*Federal Trade Commission*).

[11] A noter la récente initiative prise par la F.T.C. à propos de deux questions de protection des données, la question du « *reasonable access for online consumers* » et l'« *adequate security* » des informations collectées par les sites web. Sur ces deux points, lire le *Final Report of the F.T.C. Advisory Committee on online access and Security*, publié le 15 mai 2000. Voir également l'étude menée par la F.T.C. à propos des *Privacy Policies* des sites web qui concluait à leur nette insuffisance et recommandait au gouvernement américain de prendre des initiatives législatives en cas d'inertie du secteur privé à améliorer la situation.

évolutions en matière de protection de la vie privée, dans des circonstances où la technologie rend de plus en plus facile le transfert et le traitement de données personnelles ». Dès lors, le projet considère en son article 1 que « *Aux fins de l'article 25, paragraphe 2, de la Directive 95/46/CE, pour toutes les activités rentrant dans le domaine d'application de la Directive, il est considéré que les 'principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée', dénommés ci-après « les principes », appliqués conformément aux orientations fournies par les QSP […], assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union européenne vers des organisations établies aux Etats-Unis si et dans la mesure où les conditions suivantes sont réunies en ce qui concerne les données à transférer :*

(a) l'organisation destinataire des données s'est clairement et publiquement engagée à observer les principes mis en œuvre conformément aux QSP ;

(b) l'organisation est soumise aux pouvoirs légaux d'un organisme public habilité à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quels que soient leur pays de résidence ou leur nationalité, en cas de non respect des principes ».

III. Examen des *Safe Harbor Principles*

19. Le Groupe de l'article 29 de la Directive dans ses réflexions et recommandations relatives à l'interprétation de l'article 25 de la Directive[12] a toujours rappelé que « *toute analyse sérieuse du niveau de protection adéquat doit s'intéresser aux deux éléments fondamentaux suivants : le contenu des règles applicables et les moyens d'assurer le respect de ces règles* ». C'est cette démarche en deux temps proposé par le Groupe de l'article 29 qui structure dès lors l'examen du texte américain en question. Quelques réflexions préliminaires s'inquiètent des limites de leur champ d'application.

A. En ce qui concerne le champ d'application des principes

20. On tient en premier lieu à souligner une absence de coïncidence entre, d'une part, l'exigence d'un contrôle du respect des principes du *Safe Harbor* par une juridiction telle que la F.T.C. et, d'autre part, le champ d'application du *Safe Harbor*. Celui-ci englobe en effet des domaines pour lesquels la F.T.C. n'apparaît pas compétente tels que, par

[12] Outre le document déjà cité note 7, on citera les documents suivants :
- Premières orientations relatives aux transferts de données personnelles vers des pays tiers. *Méthodes possibles d'évaluation du caractère adéquat de la protection*, Doc. Réfl. adopté par le Groupe le 26 juin 1997, DG. XV D/5020/97-FR-final.
- *Judging industry self-regulation : when does it make a meaningful contribution to the level of data protection in a third country ?*, Working document adopted by the W.P. on 14 janv. 1998, DGXV D/5057/97 final, W.P. 7.
- *Preliminary on the use of contractual provisions in the context of transfers of personal data to third countries*, Working Document, DG XV, D/5005/98 final, W.P. 9.
- *Opinion 1/97 on Canadian initiatives relating to standardization in the field of protection of privacy*, DG XV/5023/97 final corr., W.P. 2.

exemple, les télécommunications, les données relatives aux employés ou les données relatives aux données pharmaceutiques[13].

21. En second lieu, les conditions d'application des *Safe Harbor Principles* se trouvent limitées par des exceptions particulièrement larges, qui incluent *« les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites* ». Ces exceptions sont à l'origine d'une incertitude en ce qui concerne le champ d'application des principes, et fragilisent le principe de sécurité juridique essentiel à l'interprétation des principes applicables.

B. En ce qui concerne le contenu

22. Si on note ci et là quelques progrès dans la formulation des principes, le lecteur européen regrettera sans doute l'absence de toute définition précise des concepts fondamentaux. Ainsi, sans prétendre être exhaustif, la notion de *donnée personnelle* est définie vaguement par référence au champ d'application de la Directive mais cette référence ne permet pas de savoir si les *Safe Harbor Principles* donneront à la notion la même portée que celle très large consacrée par l'article 2 a). La notion de *tiers* n'est pas elle-même définie. Aussi peut-on se demander si celle de *consentement*, fondamental dans le principe 2 [« Choix (*choice*) »], requiert les mêmes conditions que celles exigées par l'art. 2 h) de la Directive, à savoir un consentement libre, explicite et informé et si ce consentement peut être retiré à tout moment. Enfin, la *donnée « sensible »*, singulièrement élargie par rapport aux versions antérieures des *Safe Harbour Principles*, se définit, elle, comme la donnée spécifiant (« *specifying* ») et non, au sens large de la Directive, comme celle « révélant » les données médicales, de santé, ethniques, raciales, etc.

23. En ce qui concerne cette fois les règles à appliquer, on souligne les insuffisances des *Safe Harbor Principles* à propos de deux principes jugés essentiels par les documents déjà cités du groupe de l'article 29 : à savoir celui de la finalité légitime (*purpose limitation principle*) et celui de l'accès[14].

> A propos de la finalité légitime

24. On souligne que son respect est *essentiel*. Il est important que les finalités fassent l'objet d'une détermination suffisante et qu'elles présentent une certaine légitimité par rapport à la mission de l'entreprise ou de l'administration dans son rapport avec les personnes concernées par les données.

[13] Il est en outre préoccupant de constater que, lorsque les recherches portant sur ces données sont financées, ne fût-ce que partiellement, par le secteur public, la législation américaine prévoit un accès libre à ces données, qui deviennent de ce fait des données publiques, non protégées, alors même qu'elles le seraient par les dispositions applicables en Europe.

[14] Pour rappel, l'étude menée pour la Commission (citée supra, note 7) distinguait 4 principes essentiels sur base des risques encourus en matière de protection des données : celui dit de l' « *individual participation* » qui consacre le droit de la personne concernée à exercer une certaine maîtrise sur l'image informationnelle qui circule à son propos ; celui dit du « *purpose limitation* » qui exige que les données soient traitées pour une finalité déterminée et légitime ; celui de la proportionnalité des données, c'est à dire la nécessité de ne traiter des données que dans la mesure où celles ci sont nécessaires à la finalité poursuivie ; celui, enfin, de la qualité des données selon lequel les données doivent être si possible exactes et mises à jour.

25. A cet égard, on ne peut se satisfaire de l'approche en vertu de laquelle toute utilisation est permise dès qu'il y a information du consommateur et que ce dernier effectue un choix, ce qui n'implique d'ailleurs pas forcément de consentement de sa part ni que le consentement constitue une garantie suffisante dans tous les cas.

26. Sur ce dernier point, nous faisons nôtres les critiques émises par le Groupe institué à l'article 29 de la Directive à propos à la fois du *Platform for Privacy Preferences* (P3P) et du *Open Profiling Standard* (OPS), lequel mettent en œuvre ces possibilités de choix[15]. La question fondamentale qui se pose est de savoir si la vie privée est négociable par « choix »[16].

27. Enfin, le devoir affirmé par le *Safe Harbor* de limiter les données traitées aux seules données pertinentes, principe qui rejoint le principe européen dit de proportionnalité, ne peut s'apprécier qu'au regard des finalités du traitement de données, ce qui suppose au préalable que ces finalités soient suffisamment déterminées. Faute de quoi, le principe de proportionnalité perd son sens. Prenons un exemple : celui des traitements assurant la gestion des employés, la Directive exigera que, parmi ces traitements, on distingue diverses finalités déterminées. Ainsi, la gestion des droits de sécurité sociale et des paiements des employés sera distinguée des traitements portant sur la gestion du temps de travail et *a fortiori* de ceux portant sur le contrôle des salariés. A chacun de ces traitements distincts correspondent des données différentes, voire des utilisateurs différents. Si la finalité n'est plus déterminée et qu'on considère que tous ces traitements concourent à la gestion du personnel au sens le plus large, les données qui, selon la Directive européenne, devraient se présenter cloisonnées, pourront être rassemblées et utilisées tantôt pour le paiement du salaire des employés, tantôt pour leur contrôle.

> En ce qui concerne le droit d'accès

28. Le document américain[17] même s'il semble affirmer le principe de l'accès, multiplie dans la FAQ 8 [« *Access principle* »] les exceptions « *Under the Safe Harbor Principles, the right of access is fundamental to privacy protection... Nonetheless, the obligation of*

[15] Sur ces « *privacy enhancing technologies* » qui permettent à l'internaute d'exprimer ses « *privacy prefe*rences » et le cas échéant de négocier lorsqu'un site web ne respecte pas de telles préférences, lire J-M. Dinant, *Platform for Privacy Preferences (P3P): finally the Convergence between Law and technology ? How far can P3P guarantee the respect of the European Data Protection Directive Requirements*, Eclip Report, disponible sur le site du *CRID*, <http://www.droit.fundp.ac.be/Textes/P3P.rtf> ; du même auteur, *Law and technology Convergence in the Data Protection Field? Electronic Threats on personal data and electronic data protection on Internet*, disponible sur le site du *CRID*, <http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf>.

[16] En d'autres termes, puis-je consentir à ce qu'autrui traite des données me concernant contre, par exemple, une réduction de prix, l'accès gratuit à Internet, etc…? Le consentement nous paraît une condition nécessaire de légitimité d'un traitement de données mais certes pas une condition suffisante. A cet égard, voir le raisonnement de T. Léonard, « E-commerce et Protection des données à caractère personnel : quelques considérations sur la licéité des pratiques nouvelles de marketing sur Internet », in *Internet et le Droit*, Colloque VUB, Nov. 1999, à paraître.

[17] On notera, par contre, les importants progrès réalisés à propos de ce que le document américain appelle le « *Data Integrity* » à savoir le principe de pertinence et l'obligation de prendre des mesures raisonnables pour s'assurer de la fiabilité des données au regard de l'utilisation prévue de celles-ci.

an organization to provide access is subject to the principle of proportionality or reasonableness and has to be tempered in certain circumstances ». S'en suit une longue liste d'hypothèses où de telles exceptions sont permises dont certaines vont bien au-delà des exceptions prévues par la Directive (cf. la longue liste reprise à la FAQ 8.5) et, surtout, ne font l'objet d'aucune obligation de motivation de la part de l'organisme qui s'en prévaut. On note en particulier (FAQ 8) l'exception propre à la défense des intérêts de l'entreprise qui collecte des données, qu'il s'agisse des coûts engendrés par la demande d'accès ou de la crainte que la demande d'accès ne serve à des concurrents. A la lecture de telles exceptions, le « droit » d'accès apparaît comme un simple intérêt à mettre en balance avec d'autres et qui est d'autant plus relevant que le traitement peut être source de décisions « *that will significantly affect the individual* ».

29. Vu le caractère vague de telles exceptions et la référence à la pondération d'intérêts, l'interprétation qui leur sera donnée est importante. La même remarque peut être adressée à propos du « *choice principle* ». Le droit d'opposition est reconnu à la personne concernée lorsque la divulgation à des tiers a lieu « *where disclosure is for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual* » ou lorsque l'utilisation est « *for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual* ». La signification des notions de traitement pour des finalités « autres » ou « incompatibles » est d'autant moins claire que, comme nous l'avons dit, le principe européen de la « *limitation purpose* », qui implique la détermination préalable des finalités, n'est pas repris.

30. On ajoute que la FAQ 12 censée expliquer le mécanisme du « *opt out* » fait référence à la seule hypothèse de l'utilisation à des finalités « *marketing* », ce qui est certes un des cas susceptibles d'être visés mais sans doute un cas non unique.

C. L"effectivité" des règles (*enforcement*)

> Remarques liminaires

31. L'« *enforcement principle* » fait l'objet, outre d'un énoncé dans le coeur même du texte, de quatre FAQ : la FAQ 6 relative à la self-certification ; la FAQ 7 à propos de la vérification ; la FAQ 5 qui suggère une coopération avec les « *European Data Protection Authorities* » et, enfin, la FAQ 11 intitulée « *Dispute Resolution and Enforcement* ».

32. Le principe de l' « *Enforcement* » affirmé par le texte des *Safe Harbor Principles* lui-même s'énonce comme suit :

> *« Effective privacy protection must include mechanisms for assuring compliance with the principle recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the principles*

and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions business make about their privacy practices are true and that privacy practices have been implemented as presented ; and (c) obligations to remedy problems arising out of failure to comply with the principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations ».

33. A la lecture du principe tel qu'exprimé par les textes américains, on s'interroge sur l'adéquation du système mis en place par les *Safe Harbor Pinciples* vis-à-vis des trois objectifs fixés par le document déjà cité du groupe de l'article 29[18] à savoir :

1. « *to deliver a good level of compliance with the rules* », ce qui suppose que les règles soient largement connues tant par les responsables de traitement que par les personnes concernées. Sur ce point, la publication des *statements* par les entreprises, leur obligation de nommer un responsable de cette déclaration et, surtout, l'obligation de publier une *privacy policy* constituent, nous semble-t-il, des initiatives intéressantes qui assurent le respect de ce premier objectif ;

2. « *to provide support and help to individuals data subjects in the exercise of their rights* » par l'intervention d'une autorité indépendante qui doit permettre aux personnes concernées de pouvoir, dans leur dialogue avec les responsables de traitement, se retrouver dans une situation de relative égalité ;

3. « *to provide appropriate redress when rules are not complied with* ». C'est le point essentiel : il s'agit, outre de permettre un accès aisé à des voies de recours en cas de violation des principes de protection des données, de constater que des sanctions suffisamment dissuasives existent telles que les responsables de traitement soient incités à ne pas enfreindre les principes.

34. Avant d'analyser cette adéquation, soulignons que l'effectivité des *Safe Harbor Principles*, loin de ne reposer que sur un système d'autorégulation[19], s'appuie en définitive essentiellement sur l'existence d'une institution juridictionnelle publique : la *Federal Trade Commission* et sur la procédure susceptible d'être intentée devant elle en cas d'« *unfair or deceiptive acts or practices in commerce* ».

35. Ainsi, l'action devant la F.T.C. apparaît comme la garantie ultime d'effectivité du système du *Safe Harbor*. On conçoit dès lors l'importance de la lettre envoyée par le Président de la F.T.C. et les craintes exprimées par nombre d'Etats devant les faibles moyens et les limites de la compétence de la F.T.C.

[18] Cf. supra, note 7.

[19] Certes, les FAQ 7 et 11 mentionnent l'existence à côté de la F.T.C. d'autres instances promues par l'autoregulation qui pourraient jouer un rôle : ainsi, les systèmes de certification par des tiers (le texte mentionne *BBB on-line*, *Trust-e*) ou des *Alternative Dispute Resolution Mechanisms*. La FAQ 11 affirme même que la F.T.C. s'est engagée à examiner en priorité les cas soumis par les organisations d'autoréglementation mais en aucune manière les *Safe Harbor Principles* n'exigent le recours à ces organismes d'autoréglementation.

36. Un tel constat amène la Commission à exprimer un doute fondamental sur l'effectivité du système. La F.T.C. a été mise en place non pour garantir, comme c'est le cas en Europe pour les « *Data Protection Authorities* », la protection du droit individuel à la vie privée mais un commerce loyal et fiable pour les consommateurs, ce qui limite *de facto* ses capacités d'intervention dans la sphère de protection des données.

37. Ensuite, la compétence de la F.T.C. en matière de protection des données, comme en témoigne le document produit par elle, est non une compétence directe (c'est-à-dire d'interprétation et de sanction d'une réglementation, fût-ce celle d'une autoréglementation comme celle du *Safe Harbor*) mais plus une compétence indirecte de comportement loyal et non trompeur d'organisations vis-à-vis des consommateurs et des tiers lorsque ces organisations émettent un type particulier de déclaration publique. L'intervention de la F.T.C. ne peut donc être que marginale, comme en témoignent l'analyse de la "jurisprudence" de la F.T.C. en la matière[20], et l'interprétation de principes et des concepts, dont pourtant nous avons souligné le caractère vague et donc l'indispensable nécessité d'interprétation, ne peut qu'être exceptionnelle. Pour être concret, si une entreprise invoque son intérêt supérieur ou le coût excessif engendré par l'accès pour refuser ce droit, dans quelle mesure la F.T.C. est-elle en droit de décider qu'il y a « *deceiptive or false statement* » alors que l'organisation s'est comportée de bonne foi et que si violation il y a, c'est par rapport à une interprétation du texte du *Safe Harbor* et non au texte lui-même.

> Analyse des FAQ concernées par le principe d' « *enforcement* »

38. Au-delà du principe exprimé de façon générale, c'est à travers la lecture des FAQ que peut s'évaluer le respect des trois objectifs considérés par le Groupe de l'article 29 comme nécessaires à l'effectivité des règles.

La FAQ n° 5 :

39. Elle institue un mécanisme auquel les organisations américaines peuvent avoir recours pour assurer l'effectivité des règles du *Safe Harbor*. Il s'agit d'un « engagement de coopération » avec les D.P.A. européennes qui se traduira par des informations et avis et s'organisera par l'intermédiaire d'un sous-groupe informel des D.P.A. établi au niveau européen. Il s'agit de la mise en place d'un mode de règlement des litiges auquel les personnes concernées pourront avoir recours et d'un engagement des organisations américaines à le respecter.

[20] Ainsi, dans les deux seules affaires *Privacy* jugées par la *F.T.C,. Geocities* du 12 févr. 1999 <http://www.ftc.gov/os/1999/9902/9823015d&o.htm> et *Reverse Action.com .Inc.* du 6 janv. 2000 <http://www.ftc.gov/opa/2000/01/reverse4.htm>, les violations étaient flagrantes. Dans l'affaire *Geocities*, cette dernière vendait les données collectées à travers le site web à des tiers, alors que la *Privacy Notice* de *Geocities* assurait qu'une telle utilisation commerciale n'existait point. Dans l'affaire *Reverse Auction*, il s'agissait d'une entreprise ayant obtenu contractuellement d'un site concurrent des informations sur les Emails des clients de ce site concurrent. Cette entreprise s'était engagée à respecter la « *Privacy Policy* » du fournisseur de ces informations, en particulier l'interdiction de *spamming*. *Reverse Auction* avait, nonobstant cet engagement, procédé largement à l'envoi de messages non sollicités.

40. On ajoutera que l'absence de coopération avec les D.P.A., de même que le non-respect des principes du *Safe Harbor*, donneront lieu à une possibilité de réclamation auprès de la F.T.C. dans le cadre de la procédure déjà décrite. Un tel système, théoriquement intéressant, se heurte cependant à l'objection de sa praticabilité. Comment les autorités européennes pourront-elles être au courant des pratiques suivies par les organisations américaines et, surtout, disposeront-elles des moyens effectifs d'investigation ? Faute de quoi, le « contrôle » des D.P.A. européennes risque d'être illusoire et de créer une fausse apparence de protection.

Les FAQ n° 6 et n° 7 :

41. Elles décrivent les systèmes d'autocertification et de vérification. L'autocertification donne lieu à une déclaration auprès du *Department of Commerce*. Cette déclaration s'accompagne de la transmission d'un certain nombre d'informations relativement sommaires[21] (nom de l'organisation, moyens de la contacter – en ce compris le nom d'une personne de contact – la « *privacy policy* » suivie et le moyen d'y accéder, l'autorité réglementaire (*statutory body*) compétente pour intervenir en cas de violation de la vie privée, le mécanisme de recours, la méthode de vérification de la conformité aux « *Safe Harbor Principles* » et les autorités de l'organisation). Pour ce dernier point, on regrette que l'organisation américaine ne doive faire mention que des activités relatives aux données personnelles reçues d'Europe.

42. Cette déclaration devrait (« *should* » dans la version anglaise du texte) être annuelle et donner lieu à une publication sur le site du *Department of Commerce*[22]. La réception du document par le *Department of Commerce* fait débuter le bénéfice de la protection dite adéquate. Le système ainsi mis en place soulève la difficulté suivante pour la personne concernée : c'est à elle de vérifier si l'organisation dont elle apprend l'existence, soit via le responsable européen de l'envoi des données, soit lors de la collecte directe des données auprès d'elle, a fait ou non déclaration de conformité. On rappellera en effet, que l'adhésion aux *Safe Harbor Principles* n'est en aucune manière obligatoire. Sa situation est donc bien différente de celle existante vis-à-vis d'organisations européennes soumises à la loi et donc présumées en état de conformité.

43. La vérification (FAQ 7) de l'autocertification est soit effectuée de manière purement interne, soit le fait d'un tiers. Dans le premier cas, une attestation doit être établie par un « représentant autorisé » (*authorized representative*) de l'organisation et doit pouvoir être produite en cas de poursuite pour non-conformité de la déclaration aux *Safe Harbor Principles*. Dans le second cas, il s'agira de méthodes d'audit, de systèmes automatiques de vérification, etc. produits par des tiers. On songe aux méthodes de labellisation déjà mises en place comme celles de Trust-e, de Webtrust, etc.

[21] On notera par comparaison avec la déclaration prévue par la Directive, qu'aucune mention n'est donnée sur les méthodes de sécurité suivies, sur les catégories de destinataires ou de données traitées, ni surtout sur les finalités précises du traitement.

[22] A noter (cf. le FAQ 6) qu'une « *misrepresentation* » créée par la déclaration au Département du Commerce permet une action pénale sur base du *False Statement Act* (18 USC § 1001).

44. Ces tiers pourront, même s'il s'agit de « *non profit organization* » être poursuivis devant la F.T.C. s'ils contribuent à des déclarations « *deceiptive or false* »[23]. Par ailleurs, ils pourront, le cas échéant, intervenir eux-mêmes d'initiative ou à la demande d'une personne concernée s'ils constatent la violation des principes du *Safe Harbor* et prendre les sanctions d'autoréglementation prévues par le label. En outre, selon la FAQ 11, la F.T.C. s'engage à analyser en priorité les recours qui pourraient ainsi être introduits par ces tiers « labellisateurs ».

La FAQ nº11 :

45. Précisément, la dernière FAQ à examiner, celle dite n°11, est fondamentale puisqu'elle concerne la résolution des litiges et la mise en vigueur des décisions. Sur ce dernier point, et pour répondre à l'exigence du Groupe 29 de l'intervention d'une *autorité indépendante*, le projet du *Department of Commerce* propose diverses solutions : la première est la coopération avec les D.P.A. européennes déjà analysée ; la deuxième est la participation à des programmes du secteur privé; la troisième, le respect des instructions d'organes officiels de surveillance chargés du traitement des plaintes de particulier et de résolution des litiges.

46. Ces trois solutions se révèlent imprécises et peu satisfaisantes vis-à-vis des exigences européennes. Le texte donne peu de précisions sur le caractère indépendant de l'autorité « *[it] is a factual question that can be demonstrated in a number of ways for example, by transparent composition and financing or a proven track record* ». En outre, se pose la question du juge de l'interprétation de ces critères vagues.

47. L'exigence européenne prévue par le groupe 29 de trouver auprès de cet organisme « *support and assistance* » n'est pas reprise. Certes, l'accès doit être, selon les *Safe Harbor Principles*, « aisé » et « à un coût raisonnable » mais ne fallait-il pas prévoir – surtout vis-à-vis d'une personne concernée située en pays lointain – que l'organisme puisse investiguer d'initiative sur simple plainte et non être, comme semble le concevoir le système américain, uniquement un lieu de résolution de litiges, ce qui exige que le consommateur développe lui-même ses griefs et les arguments.

48. Enfin, la FAQ 11 émet un souhait que la Commission voudrait voir transformer en une obligation : l'instance de recours indépendante (*independant recourse mechanism*) *devrait* publier son interprétation des *Safe Harbor Principles*. Outre l'emploi regrettable du mot « devrait », se pose la question de l'unité d'interprétation des *Safe Harbor Principles* et de la façon dont certaines autorités dites indépendantes, moins rigoureuses, pourraient attirer les organismes américains soucieux d'obtenir à un moindre prix un brevet de protection adéquate. Ce risque est d'autant plus sérieux qu'il n'existe *a priori* aucun contrôle officiel de l'interprétation des principes dont on a souligné le caractère

[23] C'est du moins, ce qu'affirme la F.T.C., normalement non compétente vis-à-vis de « *non profit organizations* » au motif que dans le cas de labellisation au sens large, l'organisme certificateur qui apporte son label, crée un bénéfice économique au profit du membre « labellisé » (cf. en ce sens, *California Dental Assac v. Fed. Trade Commission*, 24 mai 1999) cité par la lettre de la F.T.C. du 29 mars 2000 en réponse aux demandes de la Commission européenne).

vague et que les critères d'indépendance sont également énoncés de manière particulièrement floue.

49. Les sanctions susceptibles d'être prononcées varient selon le degré de gravité de la non conformité. Le principe est que la sanction doit être suffisamment rigoureuse pour garantir le respect des principes du *Safe Harbor*. Nombre d'exemples sont donnés : retrait du label, dédommagement financier[24], publicité donnée à la constatation de la non conformité. Mais le *Safe Harbor* ne précise pas comment une personne concernée pourra forcer la décision de cette « autorité indépendante » agissant comme un « *Alternative Dispute Recourse Mechanism* » (A.D.R.) et comment il pourrait le cas échéant recourir contre une telle décision.

50. La décision de l'A.D.R. « peut » ou « devrait » (*should*) faire l'objet d'une communication au département du commerce et à la F.T.C. Aucune obligation n'existe à cet égard. Dès lors, la Commission insiste sur l'emploi répété du mot « *should* » (devrait) qui dans la plupart des cas devrait être remplacé par les mots « *must* » ou « *has to* ». Rien n'est dit sur les méthodes d'investigation de l'autorité indépendante vis-à-vis des organismes incriminés.

51. Plus grave, se pose la question du moment de la perte du bénéfice de la « protection adéquate ». La notion de « non respect » persistant (*persistent failure to comply*) est peu claire à cet égard. Il semble en tout cas que c'est la notification au département du Commerce et la publication de cette « *non compliance* », après un dernier délai de réponse (30 jours) laissé à l'organisme pour faire valoir son argument, qui entraînera la perte du bénéfice de la protection adéquate.

52. Enfin, des doutes peuvent être élevés sur l'effectivité de certaines sanctions. Que se passe-t-il si l'organisme incriminé refuse de modifier ses pratiques ou de dédommager les victimes de ses agissements ? Certes, existe la possibilité de recours devant la F.T.C. et la dénonciation par l'organisation de la « *persistant failure to comply* » mais, entre-temps, la personne concernée verra l'infraction se poursuivre.

53. L'intervention de la F.T.C. s'opère dans un second temps dans la mesure où, comme elle le reconnaît expressément dans sa lettre, ses moyens sont limités et que, d'autre part, elle donnera la préférence aux cas soumis par les organisations d'autoréglementation.

54. Il est à noter que la F.T.C., si elle dispose certes d'un pouvoir d'injonction (cessation de pratiques), ne pourra prononcer elle-même des sanctions pénales ou civiles et devra se tourner vers d'autres instances juridictionnelles pour les obtenir[25]. A cet égard, se pose la question du droit des personnes concernées d'obtenir réparation pour un

[24] Il semble que la jurisprudence américaine exclut la prise en considération des dommages moraux, ce qui est regrettable dans la mesure où l'infraction aux règles de protection des données « causera » rarement un dommage financier mais bien souvent une atteinte à la réputation ou à l'image d'une personne.

[25] Sur ce point, le lecteur trouvera des renseignements utiles sur la jurisprudence américaine et le « *right to recover damages for invasion of personal privacy* » in S. Ginder, « Lost and Found in Cyberspace : Informational Privacy in the Age of the Internet », 34 *S.D.L. Rev.* 1153 (1997).

préjudice moral. Cette question est importante dans la mesure où la preuve d'un dommage financier est rarement possible. Il en est ainsi dans le cas de réception d'un mail non sollicité. Comme on le sait, la jurisprudence européenne accueille les réclamations fondées sur l'existence d'un dommage purement moral.

Conclusion

55. Sans nier que les *Safe Harbor Principles* présentent une solution audacieuse et, dans un certain sens, pleine de promesses, nous émettons des réserves à propos de l'adéquation de la protection que pourraient apporter des *Safe Harbor Principles* et la déclaration par un organisme public ou privé de leur respect.

Ces réserves sont motivées comme suit :

1) L'étendue du champ d'application reste floue et sujette à interprétation ;

2) Les principes du *Safe Harbor* ne concernent que les données couvertes par la Directive et non l'ensemble des données traitées par les organisations américaines. Ils introduisent dès lors, pour les données européennes, un régime d'exception qui risque d'être mal connu et peu respecté dans les faits ;

3) Les principes du *Safe Harbor* méconnaissent le principe de la finalité déterminée et légitime. Cette méconnaissance introduit des risques quant aux conditions d'application des autres principes ;

4) Les principes du *Safe Harbor* donnent au droit d'accès une portée trop relative et laissent dès lors aux organisations la possibilité d'échapper trop facilement à leur devoir de transparence ;

5) L'application des principes du *Safe Harbor* repose sur la « jurisprudence » ou l'intervention de multiples organes d'autoréglementation dont aucune autorité officielle ne garantit l'unité d'interprétation. En particulier, la compétence de la F.T.C. est trop indirecte en la matière pour la garantir ;

6) L'effectivité du respect des *Safe Harbor Principles* repose sur des mécanismes compliqués dont la qualité de certains est peu évidente. En particulier, l'autocertification par l'organisation elle-même est certes entourée de garanties quant aux possibilités de contestation de la conformité auprès d'autorités indépendantes, mais la qualité d'indépendance de ces autorités est peu définie et la manière dont les organisations sont soumises à ces organisations, non précisée.

7) De manière générale, l'approche américaine repose sur l'intervention des institutions privées « d'*Alternative Dispute Resolution* » dont on ne peut que constater qu'elles sont au début de leur existence, que leur fonctionnement est dès lors peu éprouvé et, enfin, que leur pouvoir d'investigation est mal précisé.

8) En définitive, on regrette que le *Safe Harbor* laisse en définitive la personne concernée démunie. C'est à elle de vérifier la situation de conformité ou non de l'organisme américain qui traite des données, c'est à elle de trouver et saisir l'autorité indépendante de contrôle apte à étudier son cas, c'est à elle de proposer les arguments de sa demande. A ce propos, une aide et un support des organisations américaines militantes des droits de l'Homme ou de défense des libertés eussent été utiles mais leur intervention n'est pas envisagée et elle risque d'être rare et peu probable, ces organisations étant créées au départ pour la défense des citoyens américains et non européens.

56. Sans doute eût-il été préférable – mais nous ne reprenons ici que le vœu exprimé par la F.T.C. dans son rapport de mai de cette année relatif à la *Privacy Online*[26] – que le législateur américain intervienne. Sans doute aussi n'était-il pas nécessaire pour lui de mettre en place un lourd arsenal législatif et administratif – le nôtre ne l'est-il pas à certains égards ? – mais plutôt d'asseoir les bases d'une auto-régulation qui a ses pleins mérites et qui doit être soutenue : « *In Doing so, however, the Commission (The F.T.C.) recognizes that industry self-regulation, as well as consumer and business education play important roles in any legislative framework, as they have in other contexts* ».

Y. P.

Note de l'éditeur sur la demande de l'auteur : le groupe 31 a donné son accord à la fin mai pour l'adoption des *Safe Harbor Principles*. Cette décision du groupe 31 a été prise à l'unanimité, ce qui est d'autant plus étonnant que le même groupe avait émis de sérieuses réserves sur cet accord au cours d'un vote purement indicatif. Le Parlement a deux mois pour remettre en cause ce document.

Yves Poullet[27]
Yves.poullet@fundp.ac.be

Professeur faculté de Droit, Directeur du CRID des FUNDP (Namur)
Expert auprès du Conseil de l'Europe, de la Commission de l'U.E et de l'Unesco

Colloque de l'IFCLA, Paris, 15 et 16 juin 2000

[26] *Privacy Online: Fair Information Practices in the ElectronicMarketplace, op. cit.*, note 8.

[27] La présente contribution n'engage que son auteur et exprime des réflexions purement personnelles. L'auteur remercie Anne-Christine Lacoste, conseillère à la Commission belge de la protection de la vie privée pour sa relecture.